UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/408,420	09/29/1999	SUNIL K. SRIVASTAVA	50325-076	4033

29989 7590 04/06/2004

HICKMAN PALERMO TRUONG & BECKER, LLP
1600 WILLOW STREET
SAN JOSE, CA 95125

EXAMINER	
ZIA, SYED	

ART UNIT	PAPER NUMBER
2131	9

DATE MAILED: 04/06/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/408,420	Applicant(s) SRIVASTAVA, SUNIL K.	
	Examiner Syed Zia	Art Unit 2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *29 September 1999*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-31* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-31* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date 7.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

This office action is in response to application filed on September 29, 1999 (Paper No. 1). Original application contained Claims 1-31. Therefor, presently Claims 1-31 are pending for consideration.

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

2. Claim1-31 rejected under 35 U.S.C. 102(b) as being anticipated by Mittra (U. S. Patent 5,748736).

3. Regarding Claim 1 Mittra teaches and describes a method for managing addition and deletion of network nodes from and to a secure multicast or broadcast group of nodes in a communications network without a single point of failure, wherein each of the nodes is associated with one of a plurality of replicated group controllers and wherein the nodes and the

group controllers are logically organized in a binary tree that represents the network nodes and the group controllers, in which leaf nodes of the binary tree represent network nodes that are joining or leaving the group, intermediate nodes represent other network nodes, and root nodes represent the group controllers (Fig.1-3), the method comprising the steps of:

joining one of the group controllers to the plurality of replicated group controllers in a local network, establishing, by one of the group controllers, a secure communication channel between one of the group controllers and another of the group controllers using a key exchange protocol, and receiving a request to add or delete a node of the group from a load balancer that is coupled to the plurality of group controllers; creating and storing a new group session key for each node in each branch of is the tree that is affected by adding or deleting the node from the group; distributing a group session key from one of the group controllers to the network nodes (col.7 line 25 to col.8 line 65).

4. Regarding Claim 11 Mittra teaches and describes computer-readable medium comprising one or more sequences of instructions for managing addition and deletion of network nodes from and to a secure multicast or broadcast group of nodes in a communications network without a single point of failure, wherein each of the nodes is associated with one of a plurality of replicated group controllers and wherein the nodes and the group controllers are logically organized in a binary tree that represents the network nodes and the group controllers, in which leaf nodes of the binary tree represent network nodes that are joining or leaving the group, intermediate nodes represent other network nodes, and root nodes represent the group

controllers, and which instructions, when executed by one or more processors, cause the processors to carry out the steps of (Fig.1-3):

- joining one of the group controllers to the plurality of replicated group controllers in a local network, establishing, by one of the group controllers, a secure communication channel between one of the group controllers and another of the group controllers using a public key exchange protocol, receiving a request to add or delete a node of the group from a load balancer that is coupled to the plurality of group controllers, creating and storing a new group session key for each node in each branch of the tree that is affected by adding or deleting the node from the group, and distributing a group session key from one of the group controllers to the network nodes (col.6 line 45 to col.61, and col.7 line 25 to col.8 line 65).

5. Regarding Claim 21 Mittra teaches and describes a method of managing addition and deletion of network nodes form and to a secure multicast or broadcast group of nodes in a communications network, wherein each of the nodes is associated with a first group controller comprising information that is replicated in a plurality of group controllers, and wherein the nodes and the group controllers are logically organized in a binary tree that represents the network nodes and the group controllers, in which leaf nodes of the binary tree represent network nodes that are joining or leaving the group, intermediate nodes represent other network nodes, and root nodes represent the group controllers (Fig.1-3), the method comprising the steps of:

joining the first group controller in a local network in which the plurality of group controllers are coupled establishing a secure channel between the first group controller and the plurality of group controllers through secure key exchange; receiving a request to add or delete a

node from a load balancer that controls distribution of requests to the group controllers generating a new group session key for each node in each branch of the tree that is affected by adding or deleting the node from the group, and distributing the group session key from the first group controller to the other group controllers over the secure channel (col.6 line 4 to col.7 line 15, col.7 line 25 to col.8 line 65, and col.13 line 57 to col.14 line 10).

6. Regarding Claim 24 Mittra teaches and describes a method for creating a secure multicast or broadcast group (Fig.1-3), the method comprising the steps of,

establishing a secure communication channel among a plurality of group controllers via a public key exchange protocol, load balancing traffic emanating from a plurality of nodes to the plurality of group controllers (col.9 line 48 to line 62); and

distributing a group session key by one of the group controllers based upon a logical arrangement of the nodes in a binary tree structure, the binary tree structure having a root node, intermediate nodes, and leaf nodes, wherein the plurality of nodes correspond to leaf nodes of the binary tree structure and the group controllers correspond to the root node (col.13 line 37 to coo.14 line 48).

7. Regarding Claim 31 Mittra teaches and describes a computer system that can manage addition and deletion of network nodes from and to a secure multicast or broadcast group of nodes in a communications network without a single point of failure, wherein each of the nodes is associated with one of a plurality of replicated group controllers and wherein the nodes and the group controllers are logically organized in a binary tree that represents the network nodes and

the group controllers, in which leaf nodes of the binary tree represent network nodes that are joining or leaving the group, intermediate nodes represent other network nodes, and root nodes represent the group controllers, the computer system comprising:

- a load balancer coupled to the group controllers for interfacing inbound service requests to a selected one of the group controllers, a bus coupled to the load balancer for transferring data, one or more processors coupled to the bus for selectively generating a group session key under control of program instructions, a memory coupled to the one or more processors via the bus, one or more sequences of program instructions stored in the memory which, when executed by the one or more processors cause the one or more is processors (col.6 line 45 to line 61) to perform the steps of:

joining one of the group controllers to the plurality of replicated group controllers in a local network, establishing, by one of the group controllers, a secure communication channel between one of the group controllers and another of the group receiving a request to add or delete a node of the group from a load balancer that is coupled to the plurality of group controllers, and creating and storing a new group session key for each node in each branch of the tree that is affected by adding or deleting the node from the group; and distributing a group session key from one of the group controllers to the network nodes channel (col.6 line 4 to col.7 line 15, col.7 line 25 to col.8 line 65, and col.13 line 57 to col.14 line 10).

8. Claims 2, 3, 5, 7, 9, 12, 13, 15, 17, 19, 22, 25, 26, 28, and 30 are rejected applied as above rejecting Claims 1, 11, 21, and 24. Furthermore, Mittra teaches and describes

- distributing a group session key further comprises: receiving a token value at the group controller to designate the group controller as having permission to selectively generate the group session key and to generate node keys associated with the intermediate nodes and the leaf nodes; and creating and storing the group session key only when the group controller has the token value (col.2 line 8 to line 20);

- distributing a group session key further comprises: determining whether the secure multicast or broadcast group has a node that is leaving the secure multicast or broadcast group, determining which of the intermediate nodes are affected by the leaving node, updating keys associated with the affected intermediate nodes, generating a new group session key, and sending the new group session key to the leaf nodes (col.8 line 36 to line 67);

- distributing a group session key further comprises: receiving a request message from one of the plurality of nodes to join the secure multicast or broadcast group, determining which of the intermediate nodes are affected by the joining node, updating keys associated with the affected intermediate nodes; generating a new group session key and a private key of the joining node; and sending a message comprising the new group session key, the private key, and the updated keys of affected intermediate nodes to the joining node (col.7 line 26 to col.8 line 35).

- receiving a request comprises receiving the request at a load balancer having a single virtual address that represents the plurality of group controllers, and establishing a secure communication channel comprises exchanging a public key of the group controller with all other group controllers in the plurality of replicated group controllers based upon optimized broadcast Diffie-Hellman protocol (col.6 line 3 to line 61).

- distributing a group session key further comprises: receiving a token value at the group controller to designate the group controller as having permission to selectively generate the group session key and to generate node keys associated with the intermediate nodes and the leaf nodes; and creating and storing the group session key only when the group controller has the token value (col.2 line 8 to line 20).

- distributing a group session key further comprises: determining whether the secure multicast or broadcast group has a node that is leaving the secure multicast or broadcast group, determining which of the intermediate nodes are affected by the leaving node, updating keys associated with the affected intermediate nodes, generating a new group session key; and sending the new group session key to the leaf nodes (col.8 line 36 to line 67).

- distributing a group session key further comprises: receiving a request message from one of the plurality of nodes to join the secure multicast or broadcast group, determining which of the intermediate nodes are affected by the joining node; updating keys associated with the affected intermediate nodes; generating a new group session key and a private key of the joining node; and sending a message comprising the new group session key, the private key, and the updated keys of affected intermediate nodes to the joining node (col.7 line 26 to col.8 line 35).

- the steps of generating the group session key only when the first group controller is designated as a master group controller that is authorized to join nodes and generate group session keys (col.12 line 50 to col. 13 line 18);

- step of distributing further comprises: circulating a token among the plurality of group controllers to designate the one group controller as having permission to selectively generate the group session key and keys associated with the intermediate nodes and the leaf nodes; and

selectively generating the group session key based upon the circulating step (col.2 line 8 to line 20, and col.13 line 39 to line 56)

- addressing the plurality of group controllers using a single virtual address (col.6 line 3 to line 61, and col.4 line 56 to col. 5 line 12).

9. Claims 4, 6, 8, 10, 14, 16, 18, 20, 23, 27, and 29 are rejected applied as above rejecting claims 3, 5, 7, 13, 15, 17, 22, 26, and 28. Furthermore, Mittra teaches and describes a system and method, wherein:

- updating keys comprises: generating a new key of a parent node of the leaving node; and encrypting the new key of the parent node with a key of a node adjacent to the parent node, and updating keys comprises performing a one way hash function on the keys associated with the affected intermediate nodes (col. 8 line 37 to line 67,and col. 13 line 59 to line 67);

- the step of load balancing network traffic that is directed from a plurality of the nodes to the plurality of group controllers (col.12 line 50 to col.13line 18);

- establishing a secure communication channel comprises: receiving a public key value that is broadcast by the Joining node, sending a collective public key value from the nodes to the joining node, computing a shared secret key; creating and storing a group shared secret key by exchanging private key values (col.12 line 60 to col.13 line 18);

- the steps of successively designating different ones of the group controllers as the master group controller in real time (col.12 line 50 to col.13 line 18).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Syed Zia whose telephone number is 703-305-3881. The examiner can normally be reached on Monday - Friday 9:00 AM to 5:00 PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

sz
March 31, 2004

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100